(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－215172
（P2000－215172A）
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ	５Ｂ０４３
			３３０Ｇ	５Ｂ０８５
Ｇ０６Ｔ　7/00		15/62	４６０	５Ｊ１０４
Ｈ０４Ｌ　9/32			４６５Ｋ	
		Ｈ０４Ｌ　9/00	６７３Ｄ	

審査請求　有　　請求項の数７　ＯＬ　（全　７　頁）　　最終頁に続く

(21)出願番号　特願平11－12452

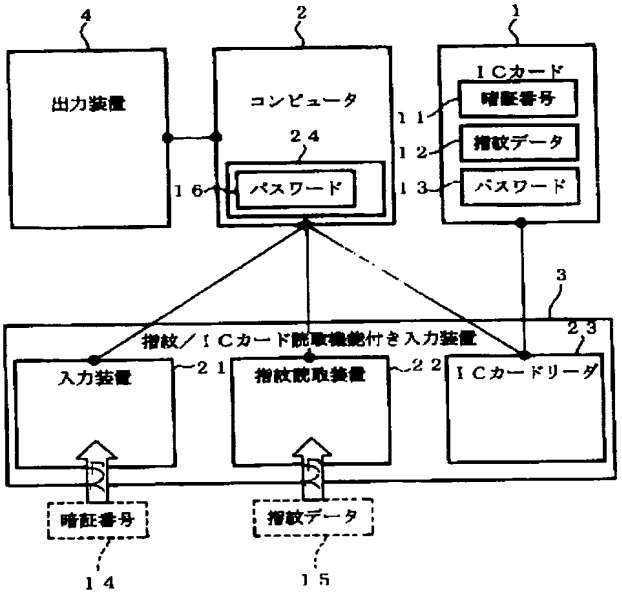
(22)出願日　平成11年１月20日(1999.1.20)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　住野　徹
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100108578
弁理士　高橋　詔男　（外３名）

Ｆターム(参考)　5B043 AA09 BA01 BA02 CA10 FA04 GA18
5B085 AE03 AE12 AE26
5J104 AA07 KA01 KA17 NA05 NA35

(54)【発明の名称】　個人認証システム

(57)【要約】
【課題】　個人認証を必要とする業務における情報機器の使用管理をより堅牢なセキュリティで実現することができる個人認証システムを提供する。
【解決手段】　情報機器２の使用者を認証するシステムであって、登録された使用者であることを特定できる生体情報１２及びパスワード１３が格納された個人認証用のカード１と、カード１に格納された生体情報１２及びパスワード１３を読み取るカード読取装置２３と、使用者から生体情報１５を読み取る生体情報読取装置２２と、カード読取装置２３から出力される生体情報１２及びパスワード１３と、生体情報読取装置２２から出力される生体情報１５及び情報機器２に格納されているパスワード１６とを照合する照合装置２４とを備えたことを特徴とする。



1

【特許請求の範囲】

【請求項１】　情報機器の使用者を認証するシステムであって、

登録された使用者であることを特定できる生体情報及びパスワードが格納された個人認証用のカードと、該カードに格納された前記生体情報及びパスワードを読み取るカード読取装置と、使用者から生体情報を読み取る生体情報読取装置と、前記カード読取装置から出力される生体情報及びパスワードと、前記生体情報読取装置から出力される生体情報及び前記情報機器に格納されているパスワードとを照合する照合装置とを備えたことを特徴とする個人認証システム。

【請求項２】　前記情報機器には、使用者が識別番号を入力する識別番号入力装置が設けられ、

前記カードには、登録された使用者であることを特定できる識別番号が格納されるとともに、格納された該識別番号と、前記識別番号入力装置より入力された識別番号とを照合する照合手段を備えたことを特徴とする請求項１記載の個人認証システム。

【請求項３】　前記生体情報は、指紋データであることを特徴とする請求項１または２記載の個人認証システム。

【請求項４】　前記指紋データは、複数の指紋データであることを特徴とする請求項３記載の個人認証システム。

【請求項５】　前記カードは、少なくとも登録された使用者であることを特定できる生体情報及びパスワードが電気信号として記憶されたＩＣカードであることを特徴とする請求項１ないし４のいずれか１項記載の個人認証システム。

【請求項６】　前記生体情報、パスワードまたは識別番号、のいずれか１つまたは２つ以上をアルゴリズムにより暗号化したことを特徴とする請求項１ないし５のいずれか１項記載の個人認証システム。

【請求項７】　前記カード読取装置と、前記識別番号入力装置と、前記生体情報読取装置とを一体化したことを特徴とする請求２ないし６のいずれか１項記載の個人認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、個人認証システムに関し、特に、情報機器起動時に使用者を認証する際に用いて好適な個人認証システムに関するものである。

【０００２】

【従来の技術】近年、コンピュータの普及が進むにつれて、データの盗難や改ざん、あるいは第三者が正当な使用者に成りすます等、コンピュータの不正使用を利用した問題が増加してきている。この問題に対し、従来より行われている対策としては、主に暗証番号のようなパスワード入力を要求するものが一般的であったが、このパスワードはあくまでも個人の知識であるために、漏洩したり他人に盗まれたりして不正使用される等の問題があった。

2

【０００３】そこで、最近では、個人情報等を格納したＩＣカードを利用した個人認証も数多く提案され、一部では実用化されてきている。このＩＣカードでは、通常、該ＩＣカードの内容をアクセスするためにはパスワード入力が必要とされているケースが多いため、上述したパスワードのみの個人認証よりは安全性が高くなっている。

【０００４】

【発明が解決しようとする課題】ところで、従来のＩＣカードを利用した個人認証では、物理的なＩＣカードと個人の知識であるパスワードを盗まれてしまうと、やはり安全性が破られてしまうという問題点があった。一方、指紋など個人の生体情報は個人毎に異なるため、個人を特定するための手段として最近注目されている。しかしながら、この生体情報を認証に用いる方法では、怪我などで生体情報が変わってしまったり、あるいは装置の性能によって誤認識される場合があるという問題点もある。

【０００５】本発明は、上記の事情に鑑みてなされたものであって、個人認証を必要とする業務における情報機器の使用管理をより堅牢なセキュリティで実現することができる個人認証システムを提供することを目的とする。

【０００６】

【課題を解決するための手段】上記課題を解決するために、本発明は次の様な個人認証システムを提供した。すなわち、請求項１記載の個人認証システムは、情報機器の使用者を認証するシステムであって、登録された使用者であることを特定できる生体情報及びパスワードが格納された個人認証用のカードと、該カードに格納された前記生体情報及びパスワードを読み取るカード読取装置と、使用者から生体情報を読み取る生体情報読取装置と、前記カード読取装置から出力される生体情報及びパスワードと、前記生体情報読取装置から出力される生体情報及び前記情報機器に格納されているパスワードとを照合する照合装置とを備えたことを特徴としている。

【０００７】請求項２記載の個人認証システムは、請求項１記載の個人認証システムにおいて、前記情報機器には、使用者が識別番号を入力する識別番号入力装置が設けられ、前記カードには、登録された使用者であることを特定できる識別番号が格納されるとともに、格納された該識別番号と、前記識別番号入力装置より入力された識別番号とを照合する照合手段を備えたことを特徴としている。

【０００８】請求項３記載の個人認証システムは、請求項１または２記載の個人認証システムにおいて、前記生体情報は、指紋データであることを特徴としている。

【０００９】請求項４記載の個人認証システムは、請求項３記載の個人認証システムにおいて、前記指紋データは、複数の指紋データであることを特徴としている。

【００１０】請求項５記載の個人認証システムは、請求項１ないし４のいずれか１項記載の個人認証システムにおいて、前記カードは、少なくとも登録された使用者であることを特定できる生体情報及びパスワードが電気信号として記憶されたＩＣカードであることを特徴としている。

【００１１】請求項６記載の個人認証システムは、請求項１ないし５のいずれか１項記載の個人認証システムにおいて、前記生体情報、パスワードまたは識別番号、のいずれか１つまたは２つ以上をアルゴリズムにより暗号化したことを特徴としている。

【００１２】請求項７記載の個人認証システムは、請求項２ないし６のいずれか１項記載の個人認証システムにおいて、前記カード読取装置と、前記識別番号入力装置と、前記生体情報読取装置とを一体化したことを特徴としている。

【００１３】

【発明の実施の形態】本発明の個人認証システムの一実施形態について図面に基づき説明する。図１は本発明の一実施形態の個人認証システムが適用されたコンピュータ・システムを示す概略構成図であり、登録された使用者であることを特定できる個人情報を格納するＩＣカード１と、使用者個人の認証を必要としプログラム制御により動作するコンピュータ（情報機器）２と、指紋／ＩＣカード読取機能付き入力装置（以下、各種機能付入力装置と称する）３と、表示機能を有しコンピュータ２のプログラム処理結果を出力または表示する出力装置４とにより構成されている。

【００１４】ＩＣカード１には、暗証番号（識別番号）１１、指紋データ（生体情報）１２、コンピュータ２起動用のパスワード１３等の各種情報が格納されている。各種機能付入力装置３は、暗証番号１４を入力する入力装置（識別番号入力装置）２１と、指紋データ（生体情報）１５を図形データとして入力する指紋読取装置（生体情報読取装置）２２と、ＩＣカード１から暗証番号１１、指紋データ１２、パスワード１３等を読み取るＩＣカードリーダ（カード読取装置）２３とを備えている。

【００１５】コンピュータ２には、使用者であることを特定できるパスワード１６が登録され、かつ、ＩＣカードリーダ２３から出力される指紋データ１２、パスワード１３等のデータと、指紋読取装置２２から出力される指紋データ１５及び該コンピュータ２に登録されているパスワード１６を照合する照合装置２４が内蔵されている。この照合装置２４により照合された結果は、出力装置４により出力または表示される。なお、前記ＩＣカード１には、暗証番号１１により指紋データ１２とパスワード１３へのアクセスを制御する保護手段、及び暗証番

号入力装置２１より入力された暗証番号１４と該ＩＣカード１に格納された暗証番号１１とを照合する照合手段が備えられている。

【００１６】次に、このコンピュータ・システムの動作について、図１及び図２に基づき説明する。まず、コンピュータの使用者は、コンピュータ２の電源を投入し（ステップＡ１）、ＩＣカード１をＩＣカードリーダ２３に挿入する（ステップＡ２）。次に、ＩＣカード１が正常に挿入されているか否かの確認が実施され（ステップＡ３）、正常に挿入されていない場合には、ＩＣカード１の挿入を要求するメッセージが出力装置４に表示される（ステップＡ４）。一方、ＩＣカード１が正常に挿入されている場合には、次のステップに進む。

【００１７】次に、ＩＣカード１に格納されている指紋データ１２やパスワード１３等をアクセスするのに必要となる暗証番号１４の入力要求メッセージが出力装置４に表示される（ステップＡ５）。使用者は暗証番号入力装置２１により暗証番号１４を入力する（ステップＡ６）。コンピュータ２はこの暗証番号１４をＩＣカードリーダ２３に送り、ＩＣカード１によって該暗証番号１４と格納されている暗証番号１１との照合が実施される（ステップＡ７）。

【００１８】暗証番号１１、１４が互いに一致しない場合は、ＩＣカード１の正当な使用者でない旨のメッセージを出力装置４に表示し、コンピュータ２の起動処理を終了する（ステップＡ８）。また、暗証番号１１、１４が互いに一致した場合は、次のステップに進む。なお、ＩＣカードリーダ２３に格納されている指紋データ１２とコンピュータ起動用パスワード１３は暗証番号１１によって保護されているため、上記照合が失敗した場合は、これ以降、内容を読み出すことは不可能である。

【００１９】コンピュータ２は、更に、使用者に指紋読取装置２２に指を置く旨のメッセージを出力装置４に表示し（ステップＡ９）、指紋データ１５をコンピュータ２に読み取る（ステップＡ１０）。次いで、コンピュータ２により上記指紋データ１５とＩＣカード１に格納されている指紋データ１２を照合する（ステップＡ１１）。　ここで、指紋データ１２、１５が互いに一致しない場合には、ＩＣカード１の正当な使用者でない旨のメッセージを出力装置４に表示してコンピュータ２の起動処理を終了する（ステップＡ８）。また、指紋データ１２、１５が互いに一致した場合は、次のステップに進む。

【００２０】最後に、コンピュータ２は、内蔵する照合装置２４により、コンピュータ起動用のパスワード１３をＩＣカード１より読み出し、コンピュータ２内に格納されているパスワード１６との照合を実施する（ステップＡ１２）。ここで、パスワード１３、１６が互いに一致しない場合には、そのコンピュータ２の正当な使用者でない旨のメッセージを出力装置４に表示し、コンピュ

ータ２の起動処理を終了する（ステップＡ１３）。また、パスワード１３、１６が互いに一致した場合は、コンピュータ２の起動処理を続行する（ステップＡ１４）。

【００２１】本実施形態のコンピュータ・システムによれば、ＩＣカード１に格納されている暗証番号１１、指紋データ１２及びコンピュータ２起動用のパスワード１３と、暗証番号入力装置２１から入力される暗証番号１４、指紋読取装置２２から入力される指紋データ１５及びコンピュータ２に登録されているパスワード１６とを照合するというように、複数レベルで個人認証を行なうことができるので、正当な使用者ではない者によるコンピュータの不正使用を防止することができる。

【００２２】また、暗証番号入力装置２１、指紋読取装置２２及びＩＣカードリーダ２３を一つの各種機能付入力装置３に統合したので、コンピュータ２と各種機能付入力装置３との間の通信を一本にまとめることができ、盗聴によるデータの漏洩等をより堅牢に防ぐことができる。

【００２３】以上、本発明の個人認証システムが適用されたコンピュータ・システムの一実施形態について図面に基づき説明してきたが、具体的な構成は本実施形態に限定されるものではなく、本発明の要旨を逸脱しない範囲で設計の変更等が可能である。例えば、本実施形態では、ＩＣカード１に１つの指紋データ１２を格納する構成としたが、ＩＣカード１に、複数（種）の指紋データ１２を格納する構成としてもよい。この場合、複数（種）の指紋データ１２を格納しておくことで、怪我などで一部の指紋データ１２が変化してしまった場合等においても、残った他の指紋データ１２を用いて個人認証を実行することができるという優れた効果がある。

【００２４】また、入力装置２１より入力する暗証番号１４、指紋読取装置２２より入力する指紋データ１５、コンピュータ２に格納されているコンピュータ起動用のパスワード１６、ＩＣカード１に格納されている暗証番号１１、指紋データ１２及びコンピュータ起動用のパスワード１３等を、既知のアルゴリズムを利用して暗号化してもよい。この場合、各装置間を行き来する個人情報を暗号化することにより、盗聴によるデータの漏洩等をより堅牢に防ぐことができるという優れた効果がある。

【００２５】

【発明の効果】以上説明した様に、本発明によれば、登録された使用者であることを特定できる生体情報及びパスワードが格納された個人認証用のカードと、該カードに格納された前記生体情報及びパスワードを読み取るカード読取装置と、使用者から生体情報を読み取る生体情報読取装置と、前記カード読取装置から出力される生体情報及びパスワードと、前記生体情報読取装置から出力される生体情報及び前記情報機器に格納されているパスワードとを照合する照合装置とを備えたので、生体情報及びパスワードを照合することで、複数レベルで個人認証を行なうことができるので、正当な使用者ではない者によるコンピュータの不正使用を防止することができる。したがって、使用者個人の認証を必要とする業務における情報機器の使用管理をより堅牢なセキュリティで実現することができる。

【図面の簡単な説明】

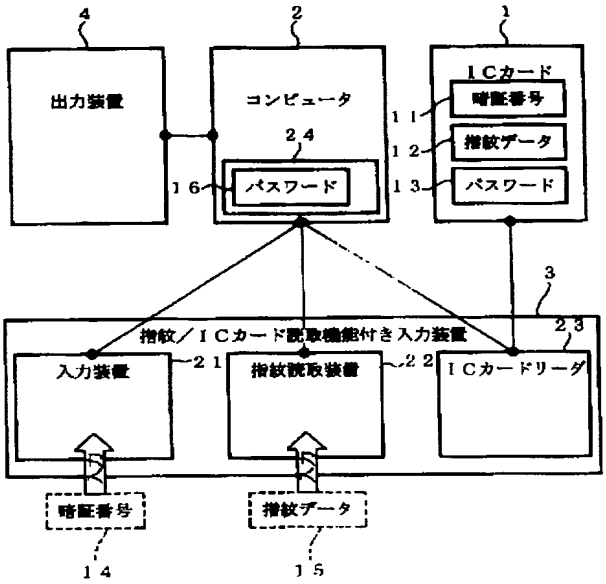
【図１】　本発明の一実施形態の個人認証システムが適用されたコンピュータ・システムを示す概略構成図である。

【図２】　本発明の一実施形態の個人認証システムが適用されたコンピュータ・システムの動作を示す流れ図である。

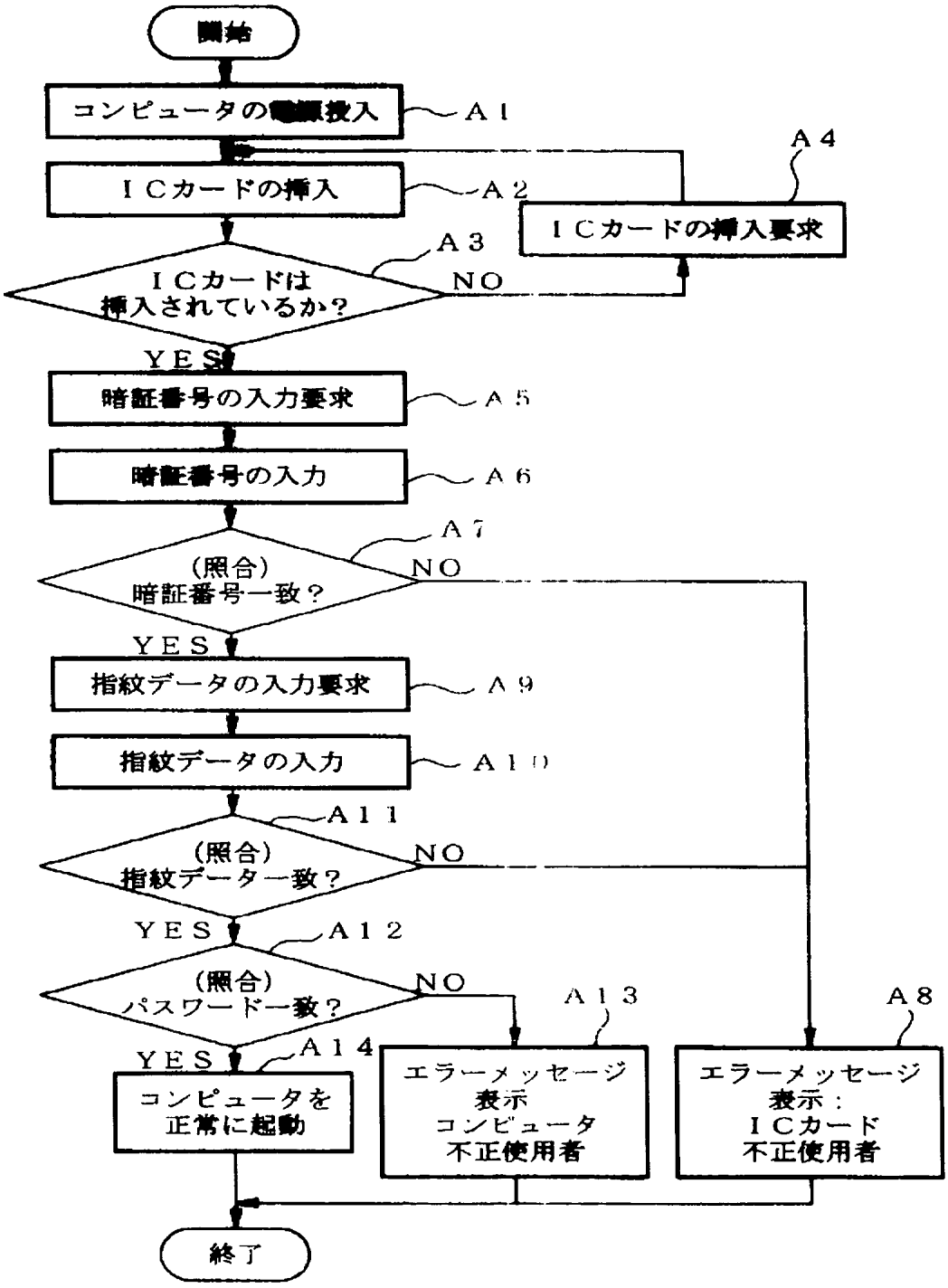
【符号の説明】

１　ＩＣカード
２　コンピュータ（情報機器）
３　指紋／ＩＣカード読取機能付き入力装置
４　出力装置
１１　暗証番号（識別番号）
１２　指紋データ（生体情報）
１３　パスワード
１４　暗証番号
１５　指紋データ（生体情報）
１６　パスワード
２１　入力装置（識別番号入力装置）
２２　指紋読取装置（生体情報読取装置）
２３　ＩＣカードリーダ（カード読取装置）
２４　照合装置

【図１】


4
2
1
出力装置
コンピュータ
ＩＣカード
暗証番号
指紋データ
パスワード
24
11
12
13
16
パスワード
3
23
指紋／ＩＣカード読取機能付き入力装置
入力装置
21
指紋読取装置
22
ＩＣカードリーダ
暗証番号
指紋データ
14
15

【図２】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
		Ｈ０４Ｌ　9/00	６７３Ｅ	
			６７３Ａ	